

### REMARKS

Reconsideration of this application is respectfully requested in view of the foregoing amendment and the following remarks.

Claims 1-54 were pending in this application. Claims 8, 12, 15, 35 and 39 have been cancelled and claims 1, 9, 10, 13, 14, 16, 20, 21, 28, 36, 37, 40-43, 45-53 have been amended hereby. Support for the amendment to the claims can be found in the now-cancelled claims as well as throughout the specification and drawings. Claims 1-7, 9-11, 13, 14, 16-34, 36-38 and 40-54 will be pending herein upon entry of this amendment. For the reasons stated below, Applicants respectfully submit that all claims pending in this application are in condition for allowance.

In the Office Action mailed January 30, 2004 the drawings were objected to, and claims 1-15 and 20-28 were rejected under 35 U.S.C. §102(e) as being anticipated by Riddle et al., U.S. Patent No. 6,457,051 (Riddle). Also, claims 16-19 were rejected under 35 U.S.C. §103(a) as being unpatentable over Riddle in view of Tang, U.S. Patent No. 6,378,126. It was further indicated that claims 29-54 were rejected for reasons similar to those of claims 1-28. To the extent these grounds of rejection might still be applied to claims presently pending in this application, they are respectfully traversed.

Examiners El Chanti and Najjar are thanked for the courtesies extended to Applicants' representative during the personal interview conducted April 21, 2004. The substance of the interview is incorporated into the following remarks.

With respect to the drawings, Applicants are filing herewith a corrected Figure 1 that includes reference number 114 and deletes reference numeral 160. In view of these minor corrections, it is believed that the objections to the drawings should be withdrawn.

Turning now to the art-based rejections, as explained during the interview, the present invention is directed to a system and method for analyzing data traveling through a network. In accordance with the present invention, a data stream is collected and resolved into logical groupings, typically made up of a plurality of packets. These packets are then assembled into respective sessions to recreate, where possible, a complete session between two end points, i.e., two computers. It is upon these assembled sessions or "session objects" that a lexical engine operates to identify one or more network events.

The present invention is particularly useful in that while it is relatively simple to identify the nature of a single packet traversing a network, it is very possible that there is significantly more information to be gleaned from an overall session composed of a plurality of packets.

Independent claims 1 and 28 have been amended to recite subject matter originally recited in the now-cancelled claims. Specifically, each of the independent claims now recites scanning network data to generate logical groupings of the network data, scanning the logical groupings to generate at least one session object, and then applying a lexical engine to the session object to identify at least one network event. Thus, as explained during the interview, the present invention may be characterized as one that operates according to a session-by-session methodology.

The characterization of the present invention sharply contrasts with that of Riddle. The focus of Riddle is to quickly classify packet flows in a network in an effort to efficiently allocate bandwidth. Significantly, Riddle is completely absent any discussion of first assembling packets into a session object and then analyzing that session object, let alone analyzing the session object with a lexical engine, as recited in each of the independent claims of the present application. Rather, Riddle appears to teach the opposite of assembling packets into sessions in that, for example, step 410 in Figure 4a and its corresponding description at column 13, line 57 – column 14 line 8 shows that once a particular packet is identified, duplicate instances having the same identifying characteristics are suppressed, in favor of keeping a count of the duplicates and a most recent time traffic with these identifying characteristics was encountered. In other words, in accordance with a network analysis tool consistent with the teachings of Riddle, it would be impossible to assemble an entire session, which is of primary importance in the present invention.

Since Riddle fails to disclose each and every element of independent claims 1 and 28, Applicants respectfully submit that the §102 rejection of the claims be reconsidered and withdrawn.

Applicants further point out that the applied Tang reference fails to overcome the deficiencies of Riddle. Accordingly, Applicants respectfully request that the §103 rejection also be reconsidered and withdrawn.

In view of the foregoing all of the claims in this case are believed to be in condition for allowance. Should the Examiner have any questions or determine that any further action is

Serial No.: 09/552,878  
Art Unit: 2157

Attorney's Docket No.: MAN0002-US  
Page 17

desirable to place this application in even better condition for issue, the Examiner is encouraged to telephone applicants' undersigned representative at the number listed below.

SHAW PITTMAN LLP  
1650 Tysons Boulevard  
McLean, VA 22102  
Tel: 703/770-7900

Date: April 27, 2004

Respectfully submitted,

ABROMAVAGE ET AL.

By:

for

Lawrence D. Eisen  
Registration No. 41,009

REG. 32,329

Attachments: Drawing Replacement Sheet

MDB/LDE/dkp